İŞLETİM SİSTEMLERİNE GİRİŞ

Öğr. Gör. Sevdanur Duran nursevdaduran@gmail.com

İŞLETİM SİSTEMLERİ GÜVENLİĞİ

- İşletim sistemleri, işlem yapma yeteneği olan araçların bütünsel bir sistem oluşturmasını ve görevlerini yerine getirmesini sağlayan yazılımlardır.

- İlerleyen başlıklarda işletim sistemlerinin güvenliğine ve olası tehditlere, zararlı yazılımlara ve sistem korunmasının nasıl olabileceği konularına yer verilmiştir.

1-İŞLETİM SİSTEMLERİ AÇIKLARI VE TEHDİTLER

- Bir işletim sistemi veya uygulamadaki güvenlik açıkları şu faktörlerden kaynaklanabilir:

- **Program hataları;** Program kodundaki bir hata, bilgisayar virüsünün cihaza erişerek cihaz kontrolünü ele geçirmesine yol açabilir,
- **Amaçlanan özellikler;** Uygulamaların sisteme erişmesini sağlayan, yasal ve belgelenmiş yöntemlerdir.

- İşletim sistemlerinin güvenlik açıkları genellikle İnternet'e bağlı olduğu durumlarda kendini gösterir.

- İnternet protokollerinden çerezlere ve kullanıcının gezinmede kullandığı tarayıcıya kadar birçok yapı, barındırdığı açıklarla sistemin tehdit edilmesine olanak tanır.

- # İnternet Protokolleri

- TCP/IP olarak bilinen, bilgi iletimi ve paylaşımının yapılmasına olanak tanıyan İnternet protokolleri de en çok tercih edilen bir diğer güvenlik açığıdır.

- (**TCP/IP (Transmission Control Protocol/Internet Protocol),** bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel isimdir.)

- TCP/IP'den kaynaklı olarak ortaya çıkabilecek zafiyetler aşağıda sıralanmıştır.

- Bir paketin bir bilgisayardan çıkıp karşı bilgisayara iletildiği yol boyunca gizlenmemesi sebebi ile paketin içeriği, yol boyunca, karşı tarafa ulaşana kadar izlenebilir ve okunabilir.
- Bir paketin kaynak adresi değiştirilebilir.
- Paketin içeriği değiştirilebilir.
- Hizmet engelleme saldırıları yapılabilir.
- Servisleri devre dışı bırakma saldırıları yapılabilir.

- **Çerezler (Cookies)**

- Çerezler, tarayıcıdan İnternet erişiminde kullanılan araca yerleşen küçük veri dosyalarıdır ve tasarımcısına göre size ait bir çok kişisel bilgiyi taşıyabilir şekilde hazırlanabilmektedir.
- Çerezler kullanılarak sisteme yetkisiz erişim sağlanılabilir.

- **Tarayıcılar**

- İşletim sistemlerinin İnternet'e ulaşım yolu web tarayıcıları aracılığıyla olmaktadır.

- İnternet erişimi engellenebilir.
- Ana tarayıcı ayarları ele geçirilerek istenilen içeriklere yönlendirilebilir.
- İşletim sistemlerine okuyucu, düzenleyici malwareler(kötü yazılım) gönderilebilir.
- Tarayıcı eklentileri ele geçirilerek arkaplanda istenildiği gibi yönlendirilebilir.

2-ZARARLI YAZILIMLAR

- İşletim sistemlerinde açık arayan ve üzerinde çalışan kullanıcı tanımlı özel programlara, dosyalara zarar veren, kişisel bilgileri tehdit eden zararlı amaçlı yazılımlar, bilişim dünyasında en çok soruna sebep olan suçlar arasında yer almaktadır. Bir çok farklı amaçla yaratılmış olan bu yazılımlar sistemin tamamen çalışmaz hâle gelmesine, kişisel bilgilerin çalınmasına, bilgi bütünlüğünün bozulmasına ve gizlilik ihlallerine kadar birçok probleme yol açmaktadır.

- **Malware (malicious software)** yani kötü amaçlı yazılım genel olarak **Truva atları**, **casus yazılımlar**, **virüsler** ve **solucanlar** olarak bilinirler.

- **Virüs ve Solucanlar**

- **Virüsler** kendini çoğaltarak kullanıcı sistemine zarar verebilen programcıklar iken **solucanlar** genellikle e-posta üzerinden kullanıcıya ulaşır.

- **Truva Atı**

- Truva atı hiçbir şekilde kendini çoğaltmaz ancak dışarıdan kullanıcıya, sisteme bulaşma yolu arar ve çalışma hızına bağlı olarak işletim sisteminde aşırı yüke neden olabilir. **Backdoor** olarak ifade edilen yapıda tasarımcısına, yüklendiği sistemde bir arka kapı açar ve sisteme ulaşmasına olanak tanır.

- **Casus Yazılımlar (Spyware)**

- Kullanıcıya ait bilgilere ulaşmaya çalışan yazılım türüdür. İstem dışı araç çubukların oluşmasına ve birçok pencerenin aynı anda açılmasına neden olabilirler.
- En çok bilinen türü **Keylogger**'dır.
- **Keylogger**, kullanıcının tuş kombinasyonlarını tutarak tasarımcısına derlediği verileri aktarır.

3-İŞLETİM SİSTEMİ GÜVENLİK MEKANİZMALARI

- Donanımlar ve yazılımlar arası bağlantıları sağlayan işletim sistemleri oldukça karmaşık yapılardır. Karmaşık yapılarla uğraşmak bilgisayar güvenliğini sağlarken karşılaşılan temel zorluklardan biridir.

- Karmaşık yapı olarak ifade ettiğimiz işletim sistemi güvenliğini bilgisayarın bütün güvenliği olarak ele alıp genel yapı için bazı güvenlik prensipleri geliştirmek ve bu prensipleri destekler nitelikte mekanizmaları işe koşmak gerekir.

- **Güvenlik Prensipleri**

- **Kişisel bir ortamın güvenliğini sağlamak adına kullanıcıların aşağıdaki gibi prensipleri benimsemesi ve uygulaması gerekmektedir;**

- İşletim sistemi girişlerinin kullanıcı adı ve parola ile korunması,
- Birden çok kullanıcı tarafından ulaşılabilen bir sistemde kişiye özel oturumların oluşturulması,
- Harici aygıtların gerekli olmadıkça kullanılmaması,

- Sisteme bağlanan harici aygıtların açılmadan önce mutlaka güvenlik taramasından geçirilmesi,
- Sistem yamalarının ve bütününün güncel tutulması,
- Kullanılan uygulama yazılımlarının yasal lisanslama modeline sahip olması (yasal olmayan lisanslama teknikleri zararlı programcıklarla sağlanmaktadır),
- İşletim sistemi için güvenlik duvarının açık tutulması,
- Zararlı yazılımları belirleyen güvenlik programlarının kurulu olması,
- Tarayıcı güvenlik ayarlarının yapılmış olması,
- Kullanıcının kullandığı e-posta servis sağlayıcılarının gelen e-postaları kontrol edebilecek güvenlik eklentilerine sahip olması
- **İşletim sistemi güvenliğini sağlamak için yeterli olacaktır.**

- **Güvenlik Mekanizmaları**

- İşletim Sistemi Oturum Güvenliği
- İşletim Sistemi Güncelleme
- Güvenlik Duvarı
- Antivirüs Programları
- Tarayıcı Güvenliği

- Oturum yönetiminin ve kullanıcı bazlı oturum kullanımlarının olması, işletim sistemi güncellemelerinin sürekli olarak denenmesi, güvenlik duvarının açık olması ve veri paketlerini kontrol etme izninin verilmiş olması, sistemi dışardan gelebilecek programcıklara karşı tarayan anti-virüs programının kurulu olması ve son olarak tarayıcı ayarlarının yapılarak, güvenlik eklentilerinin kurulmuş olması yararlanılabilecek güvenlik mekanizmaları olarak ön plana çıkmaktadır.

Kaynakça

- Doç. Dr. Mehmet FIRAT, Ders Notları